HARNESSING CYBER-TECHNOLOGY'S HUMAN POTENTIAL

BY LIEUTENANT COLONEL (P) PATRICK DUGGAN

Is the U.S. military fully harnessing the power of Cyber-technology for its human potential in conflict? Are strategists thinking differently about innovating technology for shaping the human aspects of military operations[1] versus developing technology for technology's sake? These are important questions to ponder in today's hyper-connected landscape. Successfully deterring or waging conflict in Cyberspace will require fresh ideas about human-technology innovation and new concepts to fuse fractured military capability. Using live-streaming technology as just one example, this article argues that the German military's inability to envision live-video's human potential in the 1930s coupled with Russia's modern day mastery of information-warfare video tactics, provides insightful lessons about military innovation at the nexus of human and Cyber. Capturing those lessons, a new concept like "swarm-stream" teams could employ aggressive offensive strategies like micro-targeting, disinformation attack and Cyber-smash mouth tactics to break an adversary's human-tech information advantage. If successfully developed, "swarm-stream" teams provide a prototype for unconventional thinking and offer strategic opportunities for tamping down conflict with humans in Cyberspace.

The Conflict-Cyberspace-Human Connection

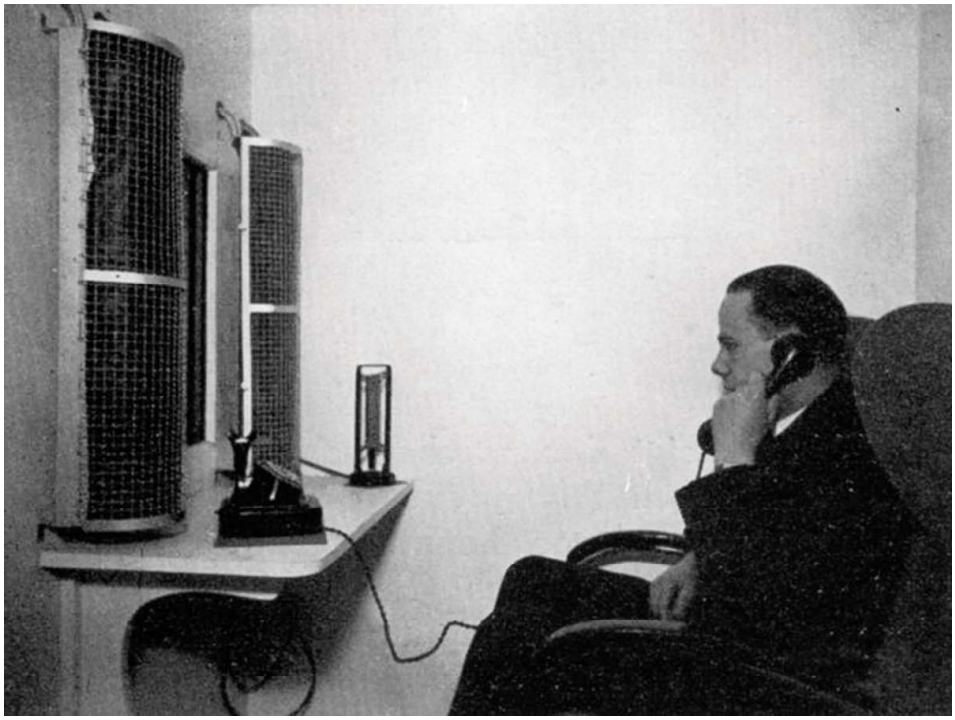
Conflict has and always will be a human enterprise. Conflict is a clash of human wills driven by passions like hatred, enmity, and fear, and is a struggle that begins and ends in the minds of men.[2] While the human nature of conflict is timeless, conflict's characteristics frequently change. Cyberspace is the latest characteristic to change and is fast becoming the dominant arena where human conflicts play out. Fortunately for humans, Cyberspace is not simply a technical abstraction or man-made domain unto itself. Instead, Cyberspace is a domain of human practice involving the actions and decisions of humans.[3] Cyberspace extends and reflects human actions, attitudes, behaviors, and decisions, and is rapidly becoming the preferred venue for how humans engage one another on a daily basis. Technologies like social media, virtual clouds, and smart devices have hyper-enabled human engagement and ushered in "a new paradigm shift in communication where everyone in the world practically has the capability to talk with everyone else simultaneously."[4] As the proliferation of increasingly advanced and inexpensive Cyber-technology continues, so too does the notion of "many to many" communication, allowing any consumer of information to also become a producer.[5] The 2015 U.S. National Military Strategy describes a global information environment where individuals have access "to more information than entire governments once possessed" and "can swiftly organize and act on what they learn, sometimes leading to violent change."[6] These complex webs of information connect humans to one another, humans to machines, and humans to the world, while providing a simultaneous, multidirectional, and information-rich domain of human practice. In short, Cyberspace is teeming with boundless human potential for the U.S. military to harness in future conflict.

1930s Germany

The act of video live-streaming is not new. Cellular and wireless technology are just recent improvements to the first public video-telephone service dating back to 1936 Germany.[7] Between 1936-1939 the German *Reichspost*, or National Post Office, laid coaxial cables linking Berlin to Nuremberg, Munich, and Hamburg providing the first public video-telephone service.[8] Groundbreaking for its time, the *Reichspost* built special booths, known as *Gegensehn-Fernsprechanlage* or visual telephone system,[9] each outfitted with eight-inch monitors[10] capable of capturing video images up to 180 pixels[11] an inch at 25 frames per second.[12] This is respectable technology considering transmission limitations of the day and as compared to the modern-day iPhone 6 which captures 441 pixels per inch at up to 60 frames per second.[13] The *Reichspost* had plans to expand the service[14] across Germany and other foreign cities but was preempted by World War II and voices advocating for other communication mediums of the time. In military circles, television was aggressively pursued for miniaturization in traditional military tasks like, visual guidance systems for bombs and rockets, remote controls, and air reconnaissance.[15] By the end of the war and despite catastrophic German losses, Allied intelligence reported on one German factory doggedly developing the technology, "producing 300 miniature cameras a month…for the still-experimental television missile guidance program."[16] Dealing another blow to early video-telephone innovation, the Nazi Minister of Propaganda, Joseph Goebbels, threw his ministry's weight behind developing televisions, where he preferred them to be built large in public settings where the general audience was believed to be more susceptible to propaganda and persuasion.[17] So in the end, the German war machine forewent early video-telephone innovation and instead repurposed its cables for more staid telegraph and broadcast television technologies.[18]

Lessons learned

Although the Germans were arguably overcome by the events and resource decisions of World War Two, the possibilities for early video-telephone's human focused innovation are valuable to consider.



VISUAL TELEPHONE SYSTEM in 1936, Dr. Georg Schubert, an engineer working for the German post office, developed the world's first public video telephone service and called it the Gegebsehn-Fernsprechanlage. *The Museum of Public Relations.*

Since the Germans made the connection between innovating television technology for traditional targeting and air reconnaissance, could the Germans have made an eventual connection between miniaturizing portable video-telephones and military espionage, unconventional warfare, and support to covert or clandestine actions? Considering the Germans had plans to expand their larger static video-telephone service abroad, could the Germans have innovated portable desk-sized versions for more human-intensive activities? The Germans could have harnessed portable video-phones to pass human intelligence, coordinate surrogate and proxy actions, direct guerrilla warfare networks, and a gamut of disruption and sabotage activities that would have benefitted from real-time visual transmission. Real-time video transmission of maps, coordinates, pictures, and added face to face context would have certainly enhanced strategic military options.

Secondly, since the Germans made the connection between employing television, movie, and radio for mass-propaganda, would they have made an eventual connection for using video-telephones as a personalized delivery means for propaganda? Considering the Germans had plans to expand their video-telephone service abroad, would the psychological impact of communication over video to select individuals have made it more compelling versus its delivery by radio or telephone?

Regardless of "what ifs" or whether miniaturized portable video-telephones would have even mattered on the whole, the key lesson for modern-day strategists is that, today, in a hyper-connected landscape filled with Cyber-technology and smart devices, strategists possess an advantage World War II Germans did not…time. Today, U.S. military strategists have the time to think differently and explore new ways to exploit human dynamics with a growing zoo of technologies...and today, countries like Russia are doing just that.

Russia in Eastern Ukraine

As recently witnessed in Eastern Ukraine, Russia's views on conflict have evolved over the last two decades, spurring the military innovation to be successful. In Spring 2014, Russia infiltrated small teams of unmarked Spetznaz, or Special Forces, across the Ukrainian border to seize government buildings and weapons armories, and then turn them over to

pro-Russian separatist militias.[19] Testifying before the Senate Armed Service Committee, former Secretary of State Madeleine Albright decried Russia's actions asserting Russia had "fundamentally changed security calculations on the continent – and marked the first time since World War II that European borders have been altered by force."[20] While Russia's choreographed information warfare campaign was powered by small SOF teams and local militias on the ground, it was virtually promoted by Russian funded "troll armies" posting pro-Russian and anti-Ukrainian comments on social media, blogs, and news sites.[21] Russia bankrolled a "$19 million dollar budget to employ 600 people whose daily tasks included commenting on 50 news articles, managing six Facebook accounts with three posts a day, managing 10 Twitter accounts, and tweeting 50 times a day.[22] At the national level, the Kremlin surged the budget of their state controlled news, Russia Today (RT), to over $300 million in 2014 with plans to increase by 41% in the future.[23] Russia masterfully orchestrated propaganda efforts like dubious on the ground "exclusive-videos," Cyber trolls, and state run media and comprehensively exploited Russian ethnicity, language, history, values, culture, and identities to fracture Ukrainian populations. The Russians vertically integrated Cyber-disinformation to systematically exploit human nature, resulting in the successful invasion of the Ukraine without the West firing a shot.

"The Russian view of information war is notably broader than any Western conception."[24] The Russian military interlaces two components, the information-technical for exploiting Cyber technologies and the information psychological for exploiting the battle of human wills.[25] The Russian evolution of information warfare theory has been poignantly captured in *Recasting Redstar* by Timothy L. Thomas of the U.S. Foreign Military Studies Office, who chronicles Russia's aggressive military reforms since the Soviet Union's demise. The author cites several prominent Russian strategists and military experts who have called for broad and comprehensive reforms to sharpen Russia's information and influence capabilities against perceived Western aggression. In particular, Dr. Igor Panarin, the head of the Institute for Political and Military Analysis Center of Military Forecasting and Russian Information Warfare, proposes a number of organizational, institutional, and training reforms to sharpen Russia's information warfare capabilities, including the development of new stand-alone "Information Special Forces."[26] These information Special Forces would execute contingency planning, preparation, and possible actions for influencing human nature under specific situations.[27] Similar proposals describe special information troops as composite teams composed of expert operators, communication personnel, journalists, writers, translators, web designers, and hackers that would leverage state and military media to wage information warfare.[28]

TROLL ARMY

A state-sponsored team of commentators, using false identities, that participate in blogs, internet forums and social media to promote propaganda with the intention of swaying opinion, undermining dissident communities or changing the perception of what is the dominant view.

Even the Russian Chief of the General Staff, Valery Gerasimov, in 2013 openly corroborated Russia's thoughts on effective modern-day conflict as "a game-changing new generation of warfare whose strategic value would exceed the "power of force of weapons in their effectiveness."[29] As the senior ranking officer in the Russian military, General Gerasimov called for the use of SOF, internal opposition, and informational actions, devices, and means to nullify enemy advantages and create a permanent operating front through the entire territory of an enemy state.[30] In other words, Russia carefully choreographs Cyber-disinformation "between the states of war and peace"[31] to exploit human tensions. As a result, Russia succeeded in the occupation of a signature partner-nation of the European Union without sparking any meaningful Western military response.

Lessons learned

Russia's military actions in Eastern Ukraine should not have surprised anyone, as their perspective on conflict was portended. "The Internet and social media are seen by Russian theorists as key game-changers in the weaponization of information."[32] Russia horizontally integrated the functions of SOF, information warfare, and Cyber in a manner that was deliberately designed to fracture Ukrainian populations. Russia methodically targeted Ukrainian human dynamics to drive wedges between social, ethnic, linguistic, and identity differences between Eastern and Western Ukrainian populations. Furthermore, Russia's evolution of military writing clearly suggest that they have restructured key military functions into composite teams at the tactical level composed of SOF, information warfare practitioners, and Cyber-technicians.

The second lesson is that Russia also vertically integrated all levels of state sponsored propaganda, often using video promulgated by Cyber. Russia kept its adversaries off balance with a persistent deluge of decentralized but vertically reinforcing propaganda. "The aim of this new propaganda is not to convince or persuade, but to keep the viewer hooked and distracted, passive and paranoid, rather than agitated to action.[33] Russia used contrived and fabricated videos employing "techniques of psychological conditioning designed to excite extreme emotions of aggression and hatred in the viewer."[34] Fast moving videos depicting violence and horrific scenes accompanied by alarming music is a form of neurolinguistics programming that can leave individuals open to suggestion.[35]

In summary, Russia succeeded in horizontally integrating key military functions at the same time they vertically integrated its state run propaganda; often, Russia personalized the psychological experience with targeted video propaganda.

Swarm Stream teams

During a Senate Armed Services Testimony in spring 2015, the USSOCOM Commander, Gen. Joseph Votel, cited Russia as "adept at avoiding conventional military responses while advancing their interests through a combination of coercion, targeted violence, and exploitation of local issues…and is systematically undermining neighboring governments and complicating international responses to its aggressive actions."[36] Gen. Votel called for new thinking on unconventional strategies to leverage the unrealized potential of Cyberspace, including the development of proficiency in social media to recruit humans to causes and the cultivation of decentralized and participatory human networks.[37] In short, it is senior officer recognition that it takes unconventional Cyber-strategies to defeat unconventional Cyber-strategies, and that the U.S. must innovate Cyber-technology for its human potential to deter or wage tomorrow's conflict.

Live-stream technology is just one of many technologies that can be innovated in an unconventional manner and should be considered in the portfolio of strategic deterrents. However, to innovate, the U.S. military must think beyond just using live-video for mission command. Today's countless video-telecommunication conferences between units, commanders, and staffs is something even a transplanted World War II-era German officer would recognize. Instead, the U.S. military should consider the concept of "swarm-stream" teams, whose real-world, real-time, human-intensive mission would be threat oriented. These teams would aggressively feed viral-video across Cyberspace. Similar to the Russians, the teams would focus on exploiting the human aspects of a given situation, but with the goal of breaking their opponent's messages, mediums, or monopoly of propaganda. The teams would actively counter, undermine, and attack an opponent's message using new tactics of their own and would be the conceptual fusing of SOF, Cyber, IO, and psychological operations functions into a truly new Cyber-unconventional capability.

Tactics

Disinformation attack: Swarm-stream teams would employ offensive disinformation attack to aggressively take down or "dox"[38] an adversary's forged videos, blogs, websites, and social media sites. A cadre of "counter-propaganda experts…would pick apart what might be called all the news unfit to print"[39] and digitally map and track an adversary's larger propaganda network. Once the teams illuminate an adversary's false information network, they could either employ low grade Cyber-tools to destroy it in private or could publicly blow the network's cover, revealing true identities and associations. Live-video would be a key tool for not just shaming the adversary, but his networks and influencers who made and disseminated them.[40]

SWARM STREAM TEAMS

A threat-oriented team of people aggressively feeding viral-video across cyberspace with the goal of breaking their opponents messages, mediums or monopoly of propaganda to actively counter, undermine and attack an opponent's message.

Another disinformation attack tactic is to flood select areas with smart mobile devices and technology. This would give civilians and partners the ability to wage a powerfully effective native and organic form of disinformation attack. Civilians and partners could video, photo, upload, and wage their own crowd-sourced, disaggregated video battles against an adversary. Any geo-tagged data would also serve as the foundation for building nonstandard domains for future options.

The last disinformation tactic is for teams to support select proxy and surrogate efforts to execute low grade Cyber-attacks against adversary websites, social media, and content generators by using less advanced customizable source codes according to specific situations.

Micro-targeting: Swarm-stream teams would employ micro-targeting, which involves the "identification and surgical engagement of specific individuals for either kinetic or non-kinetic means."[41] Teams would penetrate and data-mine information relating to individuals to better understand what actions would have the desired effect for a given individual, as well as locate a given individual with precision.[42] Non-kinetic micro-targeting for individuals would leverage multi-disciplined pools of information focused on teasing out any human dynamics to discover an individual's video-based vulnerabilities. Micro-targeting at the tactical level would employ mobile applications, analytic tools, and smart technology for the diffusion of timely information into viral-video fed Cyber-streams.

Cyber-smash mouth: Finally, swarm-stream teams would employ unconventional Cyber-smash mouth tactics, which colloquially, "takes the gloves off" in a variety of areas. Teams could build and employ surrogate, internally sourced, or outsourced communities of practice that attack an adversary's messages in native language with spam and viral-video with the intent of fragmenting polarized identities. As messages and video are repeatedly viewed and forwarded across an adversary's network, the intent is to cause shame, demoralize, and traumatize leadership into taking psychologically impaired actions. The team would attempt to undermine an adversary's credibility, influence, and power to the point of leadership neutralizing themselves, as well as, encourage adversaries to turn on their own members in search of "moles" and "traitors."

Conclusion

Conflict remains a violent struggle amongst and between people that is only getting more complex. The U.S. military must update its mindset about technology innovation if it hopes to harness Cyberspace's vast human potential for future conflict. Creating strategic opportunities may require the consolidation of fractured capabilities across the disparate functions of SOF, information warfare, psychological operations, and Cyber into new elements like "swarm-stream" teams, which are but one prototype of future human-tech innovation. As witnessed by Russia's recent actions, successfully waging or deterring conflict will require mastering the human-aspects of Cyberspace. **SW**

Lt. Col. (P) Pat Duggan *is a career Special Forces officer currently assigned in the National Capital Region and has written several articles on Cyber-enabled Special Warfare to include, 2015's Chairman of the Joint Chiefs of Staff Award Paper for National Defense and Military Strategy.*

Notes

1. The Joint Concept for Human Aspects of Military Operations (JC-HAMO) is an ongoing inter-service initiative comprised of the U.S. Army, Marine Corp, and USSOCOM that is championing DOD efforts to emphasize human factors in warfare. "The Joint Force must undertake long-term efforts to understand and influence relevant actors, examining the social, cultural, physical, informational, and psychological elements that shape human decision-making and behavior.
2. U.S. Department of the Navy, *Warfighting*, Marine Corp Doctrine Publication 1 (Washington, DC: U.S. Department of the Navy, June, 1997), 13-17. http://www.marines.mil/Portals/59/Publications/MCDP%201%20Warfighting.pdf (accessed August 2, 2015)
3. Dorothy E. Denning. "Rethinking the Cyber Domain and Deterrence." *Joint Forces Quarterly* 77, (April 1, 2015): 8. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/581864/jfq-77-rethinking-the-cyber-domain-and-deterrence.aspx (accessed August 2, 2015)
4. Richard B. Davenport, *Networked Mediated Influence 2.0.*, Military Thesis (Leavenworth, KS: U.S. Command and General Staff College, December 2014) 32. http://cgsc.contentdm.oclc.org/cdm/singleitem/collection/p4013coll2/id/3265 (accessed August 2, 2015)
5. Ibid., 73.
6. U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015*, Joint Publication (Washington, DC: U.S. Joint Chiefs of Staff, June, 2015), 1. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf (accessed August 2, 2015)
7. "The Invention of the Video Phone." The Museum of Public Relations, Baruch College, City University of New York. June 4, 2015, 1. http://www.prmuseum.org/blog/2015/6/4/the-invention-of-the-video-phone (accessed August 2, 2015)
8. German Television Museum Wiesbaden, "For Better Understanding, Television Broadcasting or Television Phone Service." http://www.fernsehmuseum.info/funkausstellung-38.html (accessed August 2, 2015)
9. "The Invention of the Video Phone." 1.
10. "The Television Intercom Connection Berlin – Leipzig." 166. http://www.oebl.de/Telefon/Bildtelefon/Funk_1936.pdf (accessed August 2, 2015)
11. Brian Edwards, "Before the Second World War Nazi Germany had Video Phones. Yes. Really," Mirror, April, 22, 2015. http://www.mirror.co.uk/usvsth3m/before-second-world-war-nazi-5538990 (accessed August 2, 2015)
12. "Telepresence 1936 Style," *The Economist*, October 12, 2010. http://www.economist.com/blogs/babbage/2010/10/worlds_first_videophone_service_1 (accessed August 2, 2015)
13. https://www.apple.com/lae/iphone-6/specs/ (accessed August 2, 2015)
14. "For Better Understanding, Television Broadcasting or Television Phone Service." 1.
15. William Uricchio, "Television's First Seventy-Five Years: The Interpretive Flexibility of a Medium in Transition." In *The Oxford Handbook of Film and Media Studies*, ed. Robert Phillip Kolker (New York: Oxford University Press, 2008), 298. http://web.mit.edu/uricchio/Public/pdfs/pdfs/oxford%20handbook.pdf (accessed August 2, 2015)
16. William Uricchio, "Storage, Simultaneity, and the Media Technologies of Modernity." in *Allegories of Communication: Intermedial Concerns from Cinema to the Digital*, ed. Jan Olsson and John Fullerton, eds. (Eastleigh: John Libbey, 2004): 134. http://web.mit.edu/uricchio/Public/pdfs/pdfs/storage,%20simultaneity,%20modernity.pdf (accessed August 2, 2015)
17. William Uricchio, "Television's First 75 Years." 298.
18. "Videophone-World's First Public Videophone Service: Germany 1936-1940." http://www.crm-toolkit.com/videophone-worlds-first-public-videophone-service-germany-1936-1940.html (accessed August 2, 2015)
19. Michael Gordon, "Russia Displays a New Military Prowess in Ukraine's East," New York Times, April 24, 2014, 2. http://nyti.ms/1hjczM3 (accessed August 2, 2015)
20. Secretary of State Madeleine Albright, *Statement to Senate Armed Services Committee: Statements, U.S. Senate*,114th Cong., 1st sess., January 29, 2015, 2. http://www.armed-services.senate.gov/imo/media/doc/Albright_01-29-15.pdf (accessed August 2, 2015)
21. Misha Japaridze, "Inside Russia's Disinformation Campaign," Defenseone.com, August 12, 2014, 3-4. http://www.defenseone.com/technology/2014/08/inside-russias-disinformation-campaign/91286/ (accessed August 2, 2015)
22. Oscar Jonsson and Robert Seely, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine," *The Journal of Slavic Military Studies*, (March 16, 2015):15. https://sakpol.files.wordpress.com/2015/03/jonsson-seely-2015-russian-full-spectrum-conflict.pdf (accessed August 25, 2014)
23. Peter Pomerantsev and Michael Weiss, *The Menace of Unreality; How the Kremlin Weaponizes Information, Culture, and Money*. (New York: Research Institute of Modern Russia, 2014), 4. http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf (accessed August 2, 2015)
24. Ibid.,12.
25. Ibid.,12.
26. Timothy L. Thomas, *Recasting Redstar: Russia Forges Tradition and Technology through Toughness*. (Leavenworth, KS: Foreign Military Studies Office, 2011), 314-315. http://fmso.leavenworth.army.mil/documents/RecastingRedStar_2015.pdf (accessed August 2, 2015)
27. Igor Panarin, "Russia: Political Elite Underestimates Needs for Information Warfare," *Voyenno-Promyshlennyy Kuryer*, October 15, 2008, 3. https://www.opensource.gov/portal/server.pt/gateway/PTARGS_0_0_200_203_121123_43/content/Display/CEP20081016548020#index=2&searchKey=19696649&rpp=10 (accessed August 2, 2015)
28. Timothy L. Thomas, *Recasting Redstar: Russia Forges Tradition and Technology through Toughness*. 316.
29. GEN Valery Gerasimov, "The Value of Science in Prediction," *Voyenno-promyshlenniy kur'yer*, February 27-March 5, 2013, 1-3. http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf (accessed August 2, 2015)
30. *Towards the Next Defense and Security Review: Part Two-NATO* (London, England: House of Commons Defense Committee Report, July 31, 2014), 13. http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/358/358.pdf (accessed August 2, 2015)
31. Ibid., 2.
32. Peter Pomerantsev and Michael Weiss. *The Menace of Unreality; How the Kremlin Weaponizes Information, Culture, and Money*. 17.
33. Ibid., 11.
34. Stephen Ennis, "How Russian TV uses Psychology over Ukraine," BBC UK, February 4, 2015. http://www.bbc.co.uk/monitoring/how-russian-tv-uses-psychology-over-ukraine (accessed August 3, 2015)
35. Ibid., 1.
36. GEN Joseph Votel, *Statement of Commander Unites States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., March 18, 2015, 7. http://fas.org/irp/congress/2015_hr/031815votel.pdf (accessed August 3, 2015)
37. Ibid., 10.
38. "Doxing," https://en.wikipedia.org/wiki/Doxing (accessed August 3, 2015)
39. Peter Pomerantsev and Michael Weiss. *The Menace of Unreality; How the Kremlin Weaponizes Information, Culture, and Money*. 6.
40. Ibid., 41.
41. Alexander Kott et al., "Visualizing the Tactical Ground Battlefield in the Year 2050: Workshop Report," Adelphi, MD,US Army Research Laboratory, June 2015. 10. http://www.arl.army.mil/arlreports/2015/ARL-SR-0327.pdf
42. Ibid., 10.